IN THE CLAIMS:

Kindly add new Claims 6-54, as follows:

6. A process for a consumer to submit secure verification information, comprising the steps of:

obtaining a secret identifier from a provider, said a secret identifier being unique to said consumer;

randomly scrambling the consumer's secret identifier with a plurality of randomly selected alphanumeric characters; and

submitting the combined randomly scrambled secret identifier and plurality of randomly selected alphanumeric characters to the provider.

7. A process according to Claim 6, wherein said submitting step is performed on the Internet.

8. A process according to Claim 6, wherein said a randomly scrambling step and said submitting step are performed on a computer network.

9. A process according to Claim 6, wherein said

randomly scrambling step and said submitting step are performed on a building security system.

10. A process according to Claim 6, wherein said submitting step is performed over a telephone system.

11. A process according to Claim 6, wherein said randomly scrambling step and said submitting step are performed in a credit or debit card verification system.

a'

12. A process according to Claim 6, wherein said randomly scrambling step and said submitting step are performed in an ATM system.

13. A process according to Claim 6, wherein said randomly scrambling step and said submitting step are performed in an phone card system.

14. A process according to Claim 6, wherein the consumer manually performs said randomly scrambling step.

15. A process according to Claim 6, further

comprising the step of the provider rejecting the submitted randomly scrambled identifier if the randomly scrambled identifier is substantially identical to a randomly scrambled identifier previously submitted to the provider.

16. A process according to Claim 6, wherein the randomly scrambling step includes the step of changing an order of alphanumeric characters in the secret identifier.

a'

17. A method of transacting a charge card purchase, comprising the steps of:

providing a user with a transaction form;

receiving from the user a credit card number and a super identifier, the super identifier comprising (i) a secret identifier unique to the user and (ii) a plurality of randomly chosen alphanumeric characters;

comparing the received super identifier with a plurality of previously received super identifiers; and

accepting the credit card transaction if the received super identifier is not substantially identical to previously received super identifiers.

18. A method according to Claim 17, wherein the charge card purchase comprises a credit card purchase.

19. A method according to Claim 17, wherein the charge card purchase comprises a debit card purchase.

20. A method according to Claim 17, wherein the charge card purchase comprises a phone card purchase.

a'

21. A method according to Claim 17, wherein the charge card purchase comprises a lottery ticket purchase.

22. A method according to Claim 17, wherein the secret identifier comprises a PIN.

23. A method according to Claim 17, wherein the randomly chosen alphanumeric characters are chosen by the user.

24. A method according to Claim 17, wherein the number of randomly chosen alphanumeric characters are the same as the number of characters in the secret identifier.

25. A method according to Claim 17, wherein the method is performed at a point of sale.

26. A method according to Claim 17, wherein the method is performed at a provider server.

27. A method according to Claim 17, wherein the method is performed over the Internet.

28. A method according to Claim 17, wherein the secret identifier is scrambled by the user using the plurality of alphanumeric characters.

a'

29. A method of carrying out a secure financial transaction, comprising the steps of:

receiving from a user (i) a request for a transaction and (ii) a super PIN which comprises a PIN scrambled with a plurality of alphanumeric characters randomly chosen by a user; and

rejecting the request if the received super PIN is substantially similar to a previously received super PIN.

30. A method according to Claim 29, wherein the rejection criteria is dependent on the Super PIN not including all of the alphanumeric characters that comprise the user's secret identifier.

31. A method according to Claim 29, wherein the rejection criteria is dependent on the Super PIN including substantially all of the plurality of randomly selected alphanumeric characters from a previous transaction.

a'

32. A method according to Claim 29, where the previously used plurality of randomly selected alphanumeric characters are stored.

33. A method according to Claim 29, where the rejection of the Super PIN validation triggers a supplementary validation activity .

34. Apparatus for a consumer to submit secure verification information including a secret identifier obtained from a provider, said a secret identifier being unique to said consumer, said apparatus comprising:

means for randomly scrambling the consumer's secret identifier with a plurality of alphanumeric characters; and

means for submitting the randomly scrambled identifier to the provider.

35. Apparatus according to Claim 34, wherein said means for submitting are coupled to the Internet.

36. Apparatus according to Claim 34, wherein said means for submitting are coupled to a computer network.

37. Apparatus according to Claim 34, wherein said means for submitting are coupled to a building security system.

38. Apparatus according to Claim 34, wherein said means for submitting are coupled to a telephone system.

39. Apparatus according to Claim 34, wherein said means for submitting are coupled to a credit card verification system.

40. Apparatus according to Claim 34, wherein said

means for submitting are coupled to an ATM system.

41. Apparatus according to Claim 34, wherein the consumer manually performs the random scrambling.

42. Apparatus according to Claim 34, wherein an automated process or device performs the random scrambling.

43. Apparatus according to Claim 34, wherein an automated process or device creates the Super PIN on behalf of the user.

44. Apparatus according to Claim 34, further comprising a provider server for rejecting the submitted randomly scrambled identifier if the randomly scrambled identifier is substantially identical to a randomly scrambled identifier previously submitted to the provider.

45. Apparatus according to Claim 34, wherein the means for randomly scrambling includes means for changing an order of alphanumeric characters in the secret identifier.

46. Apparatus for transacting a charge card transaction, comprising:

means for receiving from the user a credit card number and a super identifier, the super identifier comprising (i) a secret identifier unique to the user and (ii) a plurality of randomly chosen alphanumeric characters;

means for comparing the received super identifier with a plurality of previously received super identifiers; and

means for accepting the credit card transaction if the received super identifier is not substantially identical to previously received super identifiers.

47. Apparatus according to Claim 46, wherein the secret identifier comprises a PIN.

48. Apparatus according to Claim 46, wherein the randomly chosen alphanumeric characters are chosen by the user.

49. Apparatus according to Claim 46, wherein the number of randomly chosen alphanumeric characters are the same as the number of characters in the secret identifier.

50. Apparatus according to Claim 46, wherein said means for receiving are disposed at a point of sale.

51. Apparatus according to Claim 46, wherein said means for receiving are disposed at a provider server.

52. Apparatus according to Claim 46, wherein said means for receiving are coupled to the Internet.

a'

53. Apparatus according to Claim 46, wherein the secret identifier is scrambled by the user using the plurality of alphanumeric characters.

54. Apparatus for carrying out a secure financial transaction, comprising:

means for receiving from a user (i) a request for a transaction and (ii) a super PIN which comprises a PIN scrambled with a plurality of alphanumeric characters randomly chosen by a user; and

means for rejecting the request if the received super PIN is substantially similar to a previously received super PIN.